IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DOINA POPESCU, individually, and on behalf of all others similarly situated, Plaintiff, v. CF MEDICAL, LLC, d/b/a CAPIO, Defendant.	Case No. **COMPLAINT — CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Doina Popescu, individually, and on behalf of all similarly situated persons, alleges the following against Defendant CF Medical, LLC, d/b/a Capio ("Defendant" or "CF Medical"), based on personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents, as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and other similarly situated individuals' ("Class Members," as defined *infra*) sensitive personally identifiable information, including their names, Social Security numbers, dates of birth, and private health information ("PII/PHI").

2. Financial Business and Consumer Solutions, Inc. ("FBCS") is a nationally licensed debt collection agency in the United States, specializing in collecting unpaid debts from consumer credit, healthcare, commercial, auto loans and leases, student loans, and utilities. FBCS received

Plaintiff's and Class Members' PII/PHI from its clients, which is used to collect debts on behalf of its clients. One of FBCS's clients is CF Medical.

3. CF Medical is a debt purchasing company that goes by the trade name Capio[1]. CF Medical "specialize[s] in funding solutions for non-performing medical accounts."[2] On information and belief, Defendant previously used debt collection company Financial Business and Consumer Solutions, Inc. ("FBCS") in connection with debt collection services.

4. By obtaining, collecting, using, and deriving a benefit from the PII/PHI of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or about April 26, 2024, FBCS announced that certain systems in its network had been subject to unauthorized access between February 14 and February 26, 2024, and the unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access ("Data Breach"). In a filing with the Office of the Maine Attorney General, FBCS confirms that the PII/PHI of 4,253,394 individuals was exposed by the Data Breach.[3]

6. Thereafter, Defendant made its own filing with the Office of the Maine Attorney General, wherein it stated that 626,396 of its current and former customers were affected by the Data Breach.[4]

7. Per Defendant's Maine AG filing, it began notifying consumers on September 26,

[1] Capio, https://capiofi.com/ (last visited Oct. 10, 2024).
[2] CF Medical, https://cfmedicalfunding.com/ (last visited Oct. 10, 2024).
[3] FBCS Data Breach Notifications, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/7e6ff931-a035-480f-a977-e11a8af7f768.html (last visited Oct. 10, 2024).
[4] CF Medical Data Breach Notifications, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/da36d572-6a30-4d0c-925b-59aa3f142a6e.html (last visited Oct. 10, 2024).

2024, stating that CF Medical's debt collection agency, FBCS, had experienced a data breach, which it discovered on February 26, 2024. Defendant informed consumers that health information may have been exposed in the Data Breach.[5]

8. Defendant failed to adequately protect Plaintiff's and Class Members' PII/PHI—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII/PHI was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' PII/PHI because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

9. Defendant also failed to adequately protect Plaintiff's and Class Members' PII/PHI by virtue of its failure to vet its vendors—here, FBCS—and ensure they were submitting PII/PHI to an entity with adequate data security practices and that its vendors were deleting or archiving inactive PII/PHI data and files.

10. Plaintiff brings this action on behalf of all persons whose PII/PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII/PHI of Plaintiff and Class Members; (ii) adequately vet its vendor for data security practices; (ii) warn Plaintiff and Class Members of FBCS's inadequate information security practices; and (iii) effectively secure hardware containing protected PII/PHI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal law.

11. Defendant disregarded the rights of Plaintiff and Class Members by intentionally,

[5] *Id.*; *see* "L01_Source.pdf"

willfully, recklessly, or negligently failing to ensure that FBCS had adequate and reasonable safeguards and measures in place to protect the PII/PHI of Plaintiff and Class Members after that information was transferred and entrusted to FBCS in order to enable FBCS to collect the debt owed by Plaintiff and Class Members to Defendant. More specifically, Defendant failed to ensure that FBCS had taken and implemented available steps to prevent an unauthorized disclosure of data, and failed to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption, storage, and destruction of data, even for internal use. As a result, the PII/PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

12. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe in any further transfers of their sensitive data to third parties and they should be entitled to injunctive and other equitable relief.

13. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of PII/PHI; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII/PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI.

14. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data

was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

II. PARTIES

15. Plaintiff Doina Popescu is a resident of Winter Garden, Florida.

16. CF Medical is a limited liability corporation with its principal place of business located in Lawrenceville, Georgia.

III. JURISDICTION AND VENUE

17. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are Class Members who are diverse from Defendant, and (4) there are more than 100 Class Members.

18. The Court has personal jurisdiction over CF Medical because it purposely availed itself of the laws of the state of Pennsylvania by operating multiple retail locations there and offering its services to residents of Pennsylvania.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to this action occurred in this District, and Defendant is subject to the Court's personal jurisdiction with respect to this action.

IV. FACTUAL ALLEGATIONS

A. *Defendant's Business*

20. As previously alleged, Defendant is a corporation that specializes in funding solutions for non-performing medical accounts.

21. Defendant is one of FBCS's clients. Plaintiff provided her PII/PHI to Defendant in connection with utilizing Defendant's services, and Defendant, in turn, provided the PII/PHI to FBCS to collect an alleged debt.

22. On information and belief, FBCS accumulates highly private PII/PHI of its clients' customers, which is used to collect debts on behalf of its clients, such as Defendant.

23. Plaintiff provided her PII/PHI to Defendant as a condition for utilizing its services, and Defendant, in turn, provided the PII/PHI to FBCS to collect an alleged debt.

24. The information held by FBCS in its computer systems at the time of the Data Breach included the unencrypted PII/PHI of Plaintiff and Class Members, as provided by Defendant.

25. Upon information and belief, FBCS made promises and representations to its clients, including Defendant, that the PII/PHI collected from them, including that of Plaintiff and Class Members, would be kept safe and confidential, that the privacy of that information would be maintained, and that FBCS would delete any sensitive information after it was no longer required to maintain it.

26. Likewise, Defendant, for its part, made implicit promises and representations to its customers, including Plaintiff and Class Members, that the PII/PHI collected from them would be kept safe and confidential, that the privacy of that information would be maintained in accordance with industry standards and the law, and that it would delete any sensitive information after it was no longer required to maintain it.

27. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII/PHI. Plaintiff and Class Members value the confidentiality of their PII/PHI and demand security to safeguard their PII/PHI.

28. Defendant had a duty to adopt reasonable measures to protect the PII/PHI of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant had a legal duty to keep its customers' PII/PHI safe and confidential.

29. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII/PHI confidential and to protect it from unauthorized access and disclosure.

30. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII/PHI. Without the required submission of PII/PHI, Defendant could not perform the services it provides.

31. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII/PHI, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' PII/PHI from disclosure.

B. *The Data Breach*

32. According to FBCS's filing with the Office of the Maine Attorney General, FBCS discovered the vulnerability on February 26, 2024, but did not notify consumers of the Data Breach until April 26, 2024.[6]

33. The Notice of Data Event, posted on the Office of the Maine Attorney General's website, provides:

> On February 26, 2024, FBCS discovered unauthorized access to certain systems in its network. This incident did not impact computer systems outside of FBCS's network. We immediately took steps to secure the impacted environment and launched an investigation with the assistance of third-party computer forensics specialists to determine the full nature and scope of the incident. The investigation determined that the environment was subject to unauthorized access between

[6] FBCS Data Breach Notifications, *supra*, note 3.

> February 14 and February 26, 2024, and the unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access. Therefore, FBCS undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it related. We are notifying you because certain information related to you may have been accessed or exfiltrated during the incident. This notification was not delayed as a result of a law enforcement investigation.[7]

34. FBCS's filing with the Office of the Maine Attorney General also specifies that FBCS's customers' names or other personal identifiers in combination with driver's license numbers or non-driver identification card numbers were acquired by an external system breach (hacking).[8]

35. In September 2024, Defendant began sending out its own notice of breach letters ("CF Medical Notice"). The CF Medical Notice states:

> **What Happened?** On February 26, 2024, FBCS discovered unauthorized access to certain systems in its network. In response, FBCS took steps to secure the impacted environment and launched an investigation with the assistance of third-party computer forensics specialists to determine the full nature and scope of the incident. The investigation determined that the environment was subject to unauthorized access between February 14 and February 26, 2024, and the unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access. Therefore, FBCS undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it related.
>
> **What Information Was Involved?** In July 2024, FCBS's review determined that some of your personal information was contained in the data involved, including your name, Social Security number. In some instances, health information may have also been involved.[9]

36. Omitted from both the Notice of Data Breach and the CF Medical Notice are the details of the root cause of the Data Breach, the vulnerabilities exploited, and the specific remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts

[7] *Id.*; *see* Notice of Data Event.
[8] CF Medical Data Breach Notifications, *supra*, note 4.
[9] *Id.*; *see* L01_Source.pdf.

have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII/PHI remains protected.

37. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

38. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, causing the exposure of PII/PHI. Nor did Defendant take the precautions and measures needed to adequately vet its vendor, FBCS, to ensure FBCS's data security protocols were sufficient to protect the PII/PHI of Defendants customers, which Defendant turned over to FBCS.

39. The attacker accessed and acquired files containing unencrypted PII/PHI of Plaintiff and Class Members. Plaintiff's and Class Members' PII/PHI was accessed and stolen in the Data Breach.

40. Plaintiff further believes her PII/PHI, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

C. *Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII/PHI*

41. CF Medical derives a substantial economic benefit from providing services to its customers, and as a part of providing those services, Defendant retains and stores the PII/PHI of individuals, including that of Plaintiff and Class Members.

42. By obtaining, collecting, and storing the PII/PHI of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known it was responsible

for protecting the PII/PHI from disclosure, and making sure the PII/PHI was safe in the hands of any vendors to which Defendant provided that highly sensitive information.

43. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII/PHI.

44. Plaintiff and Class Members relied on Defendant to keep their PII/PHI confidential and maintained securely, to use this information for business purposes only, to provide the information to trusted and secure vendors and other third parties, and to make only authorized disclosures of this information.

45. Defendant could have prevented this Data Breach by properly securing the PII/PHI of Plaintiff and Class Members and ensuring that their vendors did the same.

46. Upon information and belief, Defendant made promises to customers to maintain and protect PII/PHI, demonstrating an understanding of the importance of securing PII/PHI.

47. Defendant's negligence in safeguarding the PII/PHI of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

D. *Defendant Knew or Should Have Known of the Risk Because Institutions in Possession of PII/PHI Are Particularly Susceptible to Cyberattacks*

48. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting institutions that collect and store PII/PHI, like Defendant, preceding the date of the Data Breach.

49. Data thieves regularly target companies that receive and maintain PII/PHI due to the highly sensitive nature of that information in their custody. Defendant knew and understood that unprotected PII/PHI is valuable and highly sought after by criminal parties who seek to illegally monetize that PII/PHI through unauthorized access.

50. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[10]

51. The exposure of PHI is also a widespread problem. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[11] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[12] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[13]

52. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known the PII/PHI it collected and maintained would be targeted by cybercriminals.

53. As custodians of PII/PHI, Defendant knew, or should have known, the importance of safeguarding the PII/PHI entrusted to it, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

---

[10] *See* 2021 Data Breach Annual Report at 6, IDENTITY THEFT RESOURCE CENTER (Jan. 2022), https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf.

[11] Adil Hussain Seh, et al., *Healthcare Data Breaches: Insights and Implications,* NATIONAL LIBRARY OF MEDICINE (May 13, 2020), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare- 08-00133/.

[12] Steve Alder, *December 2019 Healthcare Data Breach Report,* THE HIPAA JOURNAL (Jan. 21, 2020), https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.

[13] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/ (last accessed July 24, 2023).

54. Defendant was, or should have been, fully aware of the unique type and the significant volume of data it provided to FBCS, and, thus, the significant number of individuals who would be harmed by the exposure of that data.

55. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII/PHI of Plaintiff and Class Members from being compromised.

56. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII/PHI of Plaintiff and Class Members, and Defendant's failure to adequately vet their vendor, FBCS.

57. The ramifications of Defendant's failure to keep secure the PII/PHI of Plaintiff and Class Members are long lasting and severe. Once PII/PHI is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

E. ***Value of Personally Identifiable Information***

58. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[15]

59. The PII/PHI of individuals remains of high value to criminals, as evidenced by the

[14] 17 C.F.R. § 248.201 (2016).
[15] *Id.*

prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[16]

60. For example, PII/PHI can be sold at a price ranging from $40 to $200.[17] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[18]

61. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[19]

62. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, payment card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach—names and Social Security numbers—is impossible to "close" and difficult, if not impossible, to change.

63. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[20]

---

[16] Anita George, *Your Personal Data Is for Sale on the Dark Web. Here's How Much it Costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[17] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[18] *In the Dark*, VPNOVERVIEW (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 8, 2024).

[19] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021).

[20] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, NETWORK WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

64. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police.

65. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[21]

F. *Defendant Failed to Comply with FTC Guidelines*

66. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

67. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating

[21] U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

68. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

69. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

70. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of their data security practices, and those of their vendors. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

71. Defendant was at all times fully aware of its obligation to protect the PII/PHI of customers, yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. *Defendant Failed to Comply with HIPAA Guidelines*

72. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164,

Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

73. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[22] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

74. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

75. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

76. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

77. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

78. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

[22] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

79. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

80. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

81. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[23]

[23] U.S. DEP'T OF HEALTH & HUMAN SERVICES, *Breach Notification Rule,* https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

82. HIPAA requires a covered entity to have and apply appropriate sanctions against patients of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

83. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

84. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[24] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[25]

H. *Defendant Failed to Comply with Industry Standards*

85. As noted above, experts studying cybersecurity routinely identify institutions like

[24] U.S. DEP'T OF HEALTH & HUMAN SERVICES, *Security Rule Guidance Material,* http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[25] U.S. DEP'T OF HEALTH & HUMAN SERVICES, *Guidance on Risk Analysis,* https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.

Defendant as being particularly vulnerable to cyberattacks because of the value of the PII/PHI which they collect and maintain.

86. Some industry best practices that should be implemented by institutions dealing with sensitive PII/PHI, like Defendant, include but are not limited to: educating all employees; strong password requirements; multilayer security including firewalls; anti-virus and anti-malware software, encryption; multi-factor authentication; backing up data; and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all these industry best practices.

87. Other best cybersecurity practices that are standard at large institutions that store PII/PHI include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

88. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

89. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

I. *Defendant Breached Its Duties to Safeguard Plaintiff's and Class Members' PII/PHI*

90. In addition to their obligations under federal laws, Defendant owed duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed duties to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the PII/PHI of Class Members.

91. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of PII/PHI in a timely manner.

92. Defendant owed a duty to Plaintiff and Class Members to properly vet all third parties to whom they provided the PII/PHI of their customers, including FBCS.

93. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

94. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

95. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of their data security practices. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to adequately vet their vendors to ensure they maintained sufficient data security practices;

b. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

c. Failing to adequately protect customers' PII/PHI;

d. Failing to properly monitor their own data security systems for existing intrusions;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to the data security guidelines set forth by HIPAA;

g. Failing to adhere to industry standards for cybersecurity as discussed above; and

h. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' PII/PHI.

96. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII/PHI by allowing cyberthieves to access their computer network and systems which contained unsecured and unencrypted PII/PHI.

97. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII/PHI.

J. *Common Injuries and Damages*

98. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII/PHI ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the

materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII/PHI; (e) invasion of privacy; and (f) the continued risk to their PII/PHI, which remains in the possession of FBCS and Defendant, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII/PHI.

K. ***The Data Breach Increases Victims' Risk of Identity Theft***

99. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

100. The unencrypted PII/PHI of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII/PHI may fall into the hands of companies that will use the detailed PII/PHI for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII/PHI of Plaintiff and Class Members.

101. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII/PHI to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft-related crimes discussed below.

102. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

103. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a

victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

104. One such example of criminals piecing together bits and pieces of compromised PII/PHI for profit is the development of "Fullz" packages.[26]

105. With "Fullz" packages, cybercriminals can cross-reference two sources of PII/PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

106. The development of "Fullz" packages means that the stolen PII/PHI from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, driver's license numbers, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI that was exfiltrated in the Data Breach, criminals may still easily create

[26] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, KREBSONSECURITY.COM BLOG (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

107. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[27]

108. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

109. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[28]

110. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-

---

[27] *Medical I.D. Theft*, EFraudPrevention, available at https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected.

[28] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

pocket costs for healthcare they did not receive to restore coverage.[29] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[30]

L. *Loss of Time to Mitigate Risk of Identity Theft and Fraud*

111. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII/PHI was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

112. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

---

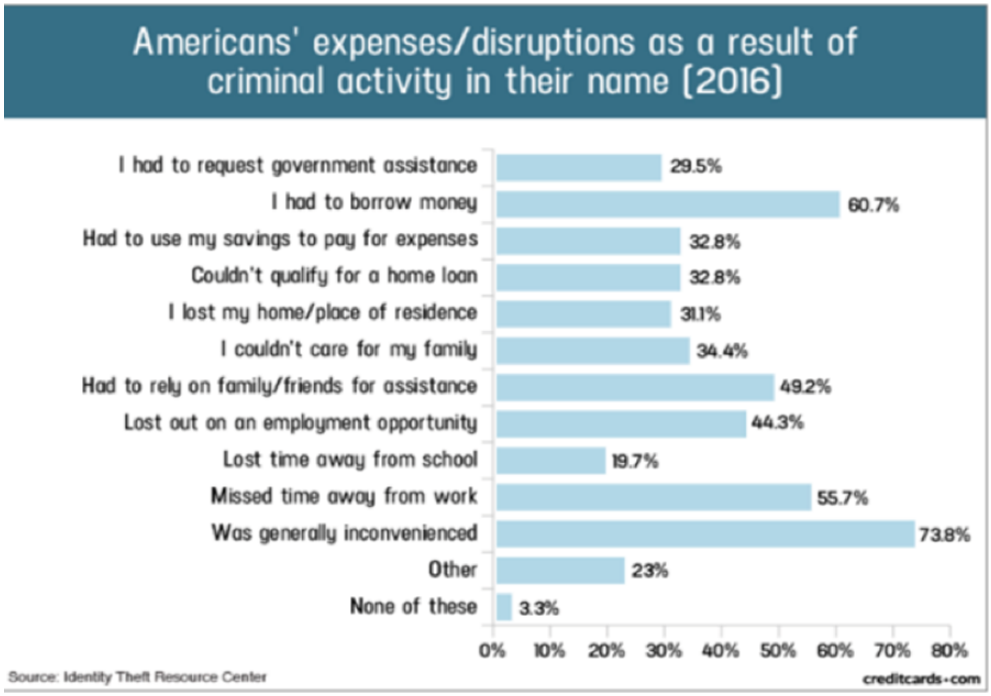
[29] *See* Elinor Mills, *Study: Medical Identity Theft is Costly for Victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.

[30] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/ (last accessed July 24, 2023).

113. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[31]

114. These efforts are also consistent with the steps the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[32]

115. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:



[31] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[32] *See* Federal Trade Commission, IDENTITYTHEFT.GOV, https://www.identitytheft.gov/Steps (last visited Oct. 8, 2024).

M. *Diminution of Value of PII/PHI*

116. PII/PHI is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that PII/PHI has considerable market value.

117. An active and robust legitimate marketplace for PII/PHI exists. In 2019, the data brokering industry was worth roughly $200 billion.[33]

118. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[34,]

119. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[35]

120. Conversely, sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[36]

121. As a result of the Data Breach, Plaintiff's and Class Members' PII/PHI, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss.

---

[33] David Lazarus, *Shadowy data brokers make the most of their cloak*, LOS ANGELES TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[34] DATACOUP, https://datacoup.com/ (last visited Oct. 8, 2024).
[35] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Oct. 8, 2024).
[36] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

Moreover, the PII/PHI is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

N. *Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary*

122. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII/PHI involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchased by criminals intending to utilize the PII/PHI for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.

123. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

124. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

125. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII/PHI.

O. *Plaintiff's Experience*

126. Upon information and belief, Defendant acquired Plaintiff's PII/PHI in the course of its regular business operations.

127. As a condition of obtaining products and/or services at CF Medical, Plaintiff was required to provide her PII/PHI to Defendant, including her name, Social Security number, and other sensitive information.

128. At the time of the Data Breach—February 14, 20243 through February 26, 2024--Defendant maintained Plaintiff's PII/PHI in its system.

129. Plaintiff Popescu is very careful about sharing her sensitive PII/PHI. Plaintiff stores any documents containing her PII/PHI in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII/PHI over the internet or any other unsecured source. Plaintiff would not have entrusted her PII/PHI to Defendant had she known of Defendant's lax data security policies.

130. Plaintiff Doina Popescu received the Notice Letter, by U.S. mail, directly from Defendant, dated September 26, 2024. According to the Notice Letter, Plaintiff's PII/PHI was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, and health information.

131. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach and changing passwords. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

132. Plaintiff suffered actual injury from having her PII/PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII/PHI; (iii) lost or diminished value of PII/PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII/PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

133. Plaintiff additionally suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach. This misuse of her PII/PHI was caused, upon information and belief, by the fact that cybercriminals are able to easily use the information compromised in the Data Breach to find more information about an individual, such as their phone number or email address, from publicly available sources, including websites that aggregate and associate personal information with the owner of such information. Criminals often target data breach victims with spam emails, calls, and texts to gain access to their devices with phishing attacks or elicit further personal information for use in committing identity theft or fraud.

134. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

135. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

136. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

137. Plaintiff Doina Popescu has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

138. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seeks certification of the following nationwide class:

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach, including all individuals who received notice of the Data Breach ("Class").

139. Excluded from the Class are Defendant and their parents or subsidiaries, any entities in which it has a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

140. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as to add subclasses, before the Court determines whether certification is appropriate.

141. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

142. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes the proposed Class includes at least 626,396 individuals whose Personal Information was compromised in the Data Breach. The

precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

143. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA;

c. Whether Defendant's conduct violated HIPAA:

d. When Defendant learned of the Data Breach;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII/PHI compromised in the Data Breach;

f. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Defendant's data security systems, prior to and during the Data Breach, were consistent with industry standards;

h. Whether Defendant owed duties to Class Members to safeguard their PII/PHI;

i. Whether Defendant breached their duties to Class Members to safeguard their PII/PHI;

j. Whether hackers obtained Class Members' PII/PHI via the Data Breach;

k. Whether Defendant had legal duties to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

l. Whether Defendant breached its duties to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;

n. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

o. Whether Defendant's conduct was negligent;

p. Whether Defendant breached express and/or implied contracts with Plaintiff and Class Members;

q. Whether Defendant was unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

144. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII/PHI, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

145. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

146. Predominance. Defendant has engaged in common courses of conduct toward Plaintiff and Class Members. For example, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

147. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

148. Class certification is also appropriate under Federal Rule of Civil Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to the Class

such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

149. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

CLAIMS FOR RELIEF

COUNT I
Negligence and Negligence Per Se
(On Behalf of Plaintiff and the Class Against Defendant)

150. Plaintiff incorporates and realleges the preceding paragraphs as if fully set forth herein.

151. Plaintiff and Class Members provided their PII/PHI to Defendant as a condition of receiving services.

152. Defendant had full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and Class Members could and would suffer if the PII/PHI were wrongfully disclosed.

153. By assuming the responsibility to collect and store this data, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

154. Defendant had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

155. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

156. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin to notify Plaintiff or Class Members of the Data Breach until September 26, 2024 despite, upon information and belief, Defendant knowing shortly after February 26, 2024 that unauthorized persons had accessed and acquired the private, protected, personal information of Plaintiff and the Class.

157. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII/PHI.

158. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

159. Defendant had and continues to have duties to adequately disclose that the PII/PHI of Plaintiff and Class Members within Defendant’s possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII/PHI by third parties.

160. Defendant breached its duties, pursuant to the FTCA and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII/PHI. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII/PHI, including in choosing its vendors

b. Failing to hold vendors with whom it shared sensitive Private Information to adequate standards of data protection;

c. Allowing unauthorized access to Class Members' PII/PHI;

d. Failing to detect in a timely manner that Class Members' PII/PHI had been compromised;

e. Failing to remove former customers' PII/PHI it was no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

161. Defendant violated Section 5 of the FTCA and HIPAA by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

162. Plaintiff and Class Members were within the class of persons the FTCA and HIPAA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm this statute was intended to guard against.

163. Defendant's violation of Section 5 of the FTCA and HIPAA constitutes negligence per se.

164. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class Members.

165. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

166. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII/PHI would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches at large corporations that collect and store PII/PHI.

167. Defendant had full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and Class Members could and would suffer if the PII/PHI were wrongfully disclosed.

168. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII/PHI of Plaintiff and Class Members, the critical importance of providing adequate security of that PII/PHI, and the necessity for encrypting PII/PHI stored on its systems.

169. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII/PHI would result in one or more types of injuries to Class Members.

170. Plaintiff and Class Members had no ability to protect their PII/PHI that was in, and possibly remains in, Defendant's possession.

171. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

172. Defendant's duties extended to protecting Plaintiff and Class Members from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

173. Defendant has admitted that the PII/PHI of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

174. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the PII/PHI of Plaintiff and Class Members would not have been compromised.

175. There is a close causal connection between Defendant's failure to implement security measures to protect the PII/PHI of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PII/PHI of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII/PHI by adopting, implementing, and maintaining appropriate security measures.

176. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII/PHI; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII/PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI.

177. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

178. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII/PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI in its continued possession.

179. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

180. Defendant's negligent conduct is ongoing, in that it still holds the PII/PHI of Plaintiff and Class Members in an unsafe and insecure manner.

181. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class Against Defendant)

182. Plaintiff incorporates and realleges the preceding paragraphs as if fully set forth herein.

183. Defendant required Plaintiff and Class Members to provide it with their PII/PHI in order to receive its products and/or services.

184. In turn, Defendant impliedly promised to protect Plaintiff's and Class Members' PII/PHI through adequate data security measures.

185. Plaintiff and Class Members accepted Defendant's offer by providing their valuable PII/PHI to Defendant in exchange for Plaintiff and Class Members receiving Defendant's products and services, and then by paying for and receiving the same.

186. Plaintiff and Class Members would not have done the foregoing but for the above-described agreement with the company.

187. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII/PHI to Defendant in exchange for, amongst other things, the protection of such information.

188. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

189. However, Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII/PHI and by failing to provide timely and accurate notice to them that their PII/PHI was compromised as a result of the Data Breach.

190. In sum, Plaintiff and Class Members have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

191. As a reasonably foreseeable result of the Data Breach, Plaintiff and Class Members were harmed by Defendant's failure to use reasonable data security measures to store their PII/PHI, including but not limited to, the actual harm through the loss of their PII/PHI to cybercriminals.

192. Accordingly, Plaintiff and Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class Against Defendant)

193. Plaintiff incorporates and realleges the preceding paragraphs as if fully set forth herein.

194. This count is brought in the alternative to Plaintiff's breach of express and/or implied contract claims.

195. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including from payments made by or on behalf of its clients for services.

196. As such, a portion of the value and monies derived from payments made by its clients for services is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

197. Plaintiff and Class Members conferred a monetary benefit on Defendant in providing it with their valuable PII/PHI.

198. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII/PHI of Plaintiff and Class Members for business purposes.

199. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII/PHI. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profit over the requisite security.

200. Defendant failed to secure Plaintiff's and Class Members' PII/PHI and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII/PHI provided.

201. Under the principles of equity and good conscience, Defendant should not be permitted to retain the benefits that Plaintiff and Class Members conferred upon it.

202. Plaintiff and Class Members have no adequate remedy at law.

203. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII/PHI; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII/PHI, which: (a) remains unencrypted and available for unauthorized

third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI.

204. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court enter an Order:

A. certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

B. Granting equitable relief and enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII/PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. Granting injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to:

   i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   ii. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all

applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to create a vendor vetting process that thoroughly analyses their vendors' data security practices to ensure they are in compliance with state and federal law and industry standards;

iv. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

v. requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII/PHI of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the PII/PHI of Plaintiff and Class Members on a cloud-based database;

vii. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Dated: October 10, 2024

Respectfully submitted,

By: */s/ Andrew Ferich*

Andrew W. Ferich (PA I.D. 313696)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Tel.: 310-474-9111
Fax: 310-474-8585
aferich@ahdootwolfson.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: 954-525-4100
ostrow@kolawyers.com

Charles E. Schaffer (PA I.D. 76259)
LEVIN SEDRAN & BERMAN, LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: 215-592-1500
cschaffer@lfsblaw.com

John A. Yanchunis*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, FL 33602
Tel: 813-223-5505
JYanchunis@forthepeople.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606

Tel: 866-252-0878
gklinger@milberg.com

Counsel for Plaintiff and the Putative Class

**pro hac vice* pending or to be filed